

Attorney Docket No. AUS920030685US1
Serial No. 10/682,402

RECEIVED
CENTRAL FAX CENTER

OCT 01 2007

I. CLAIM AMENDMENTS

Please amend the claims as indicated in the following listing:

1. (currently amended) An apparatus comprising:

a firewall, having a processor and a memory,

wherein the firewall is part of a router that creates a plurality of Virtual Local Area

Networks using a network switch;

wherein the network switch is connected to the firewall;

wherein the memory contains a Virtual Local Area Network rules table;

wherein the Virtual Local Area Network rules table allows an administrator to designate a trust level for each of the plurality of Virtual Local Area Networks;

wherein only the firewall is used to protect each of the plurality of Virtual Local Area

Networks in accordance with a designated trust level;

wherein the designated trust level is a security level associated with a particular set of rules in the firewall;

wherein a residence time is the time required for the firewall to analyze and either permit or deny a packet; and

wherein the designated trust level reduces the residence time of the packet in the firewall.

2. (previously amended) The apparatus of claim 1 wherein the Virtual Local Area Network rules table further comprises:

defining the relationship between the trust levels, the rules, and the plurality of Virtual Local Area Networks.

3. (previously amended) The apparatus of claim 2, wherein the firewall further comprises: a configuration program, wherein the configuration program allows a user to add, delete, or

Attorney Docket No. AUS920030685US1
Serial No. 10/682,402

modify the Virtual Local Area Network rules table and a plurality of trust levels in the Virtual Local Area Network rules table.

4. (previously amended) The apparatus of claim 2, wherein the firewall further comprises: a security program, wherein the security program analyzes a packet and determines if the Virtual Local Area Network rules table permits or denies the packet.
5. (currently amended) The apparatus of claim 4, wherein the security program comprises:
 - instructions for determining a destination of the packet;
 - instructions for determining an appropriate rule to use to analyze the packet using the Virtual Local Area Network rules ~~table~~-table;
 - instructions for analyzing the packet using the appropriate rule;
 - instructions for determining if the packet is permitted under the appropriate rule;
 - responsive to a determination that the appropriate rule permits the packet, instructions for permitting the packet; and
 - responsive to a determination that the rules deny the packet, instructions for denying the packet.
6. (previously amended) The apparatus of claim 5, wherein the security program further comprises: responsive to a determination that the rules do not permit or deny the packet, instructions for denying the packet.
7. canceled.
8. (currently amended) A router comprising:
 - a switch connected to a firewall and a plurality of computer networks; and
 - wherein the firewall allows an administrator to configure a plurality of trust levels and to associate a trust level with each of the plurality of computer networks;

Attorney Docket No. AUS920030685US1
Serial No. 10/682,402

wherein the firewall serves each of the plurality of computer networks in accordance with the trust level associated with each of the plurality of computer networks;

wherein the trust level is a security level associated with a particular set of rules in the firewall;

wherein a residence time is the time required for the firewall to analyze and either permit or deny a packet; and

wherein the trust level reduces the residence time of the packet in the firewall.

9. (original) The router of claim 8 wherein the switch comprises a sub-switch, the sub-switch being assigned one of a plurality of trust levels.
10. (original) The router of claim 8 wherein the firewall analyzes a packet using some of the rules; and wherein the rules used in the lower trust levels are excluded from the rules used to analyze the packet.
11. (original) The router of claim 8, wherein the firewall further comprises: a configuration program, wherein the configuration program allows a user to add, delete, or modify the rules and trust levels in the table.
12. (currently amended) The router of claim 8, wherein the firewall further comprises: a security program, wherein the security program analyzes ~~at~~the packet and determines if the rules permit or deny the packet.
13. (original) The router of claim 12, wherein the security program comprises:
 - instructions for determining the sub-switch location of the packet;
 - instructions for determining a source of the packet;
 - instructions for determining a destination of the packet; and
 - instructions for determining if the packet is attempting to go to a higher trust level;

Attorney Docket No. AUS920030685US1
Serial No. 10/682,402

responsive to a determination that the packet is not attempting to go to a higher trust level, instructions for permitting the packet.

14. (original) The router of claim 13, wherein responsive to a determination that the packet is attempting to go to a higher trust level, the security program further comprises:

instructions for determining the appropriate rules to use to analyze the packet using the table;

instructions for analyzing the packet using the rules;

instructions for determining if the packet is permitted under the rules;

responsive to a determination that the rules permit the packet, instructions for permitting the packet; and

responsive to a determination that the rules deny the packet, instructions for denying the packet.

15. (original) The router of claim 14, wherein the security program further comprises: responsive to a determination that the rules do not permit or deny the packet, instructions for denying the packet.

16. (original) The router of claim 8 wherein the firewall further comprises: a table defining the relationship between the trust levels, the rules, and the computer networks.

17. (currently amended) A method for analyzing a packet using a firewall which creates a plurality of trust levels for a plurality of computer networks, the method comprising:

using a single router containing the firewall to service each of the plurality of computer networks by performing the steps of:

determining the destination of the packet;

Attorney Docket No. AUS920030685US1
Serial No. 10/682,402

accessing a plurality of rules;
determining the appropriate rules to use to analyze the packet;
analyzing the packet using the rules;
determining if the packet is permitted under the rules;
responsive to a determination that the rules permit the packet, permitting the packet;

and

responsive to a determination that the rules deny the packet, denying the packet;
wherein a trust level is a security level associated with a particular set of rules in the

firewall;

wherein a residence time is the time required for the firewall to analyze and either
permit or deny the packet; and

wherein the trust level reduces the residence time of the packet in the firewall.

18. (original) The method of claim 17 further comprising: responsive to a determination that the rules do not permit or deny the packet, denying the packet.

19. (currently amended) The method of claim 17 wherein a table defines the relationship between the plurality of trust levels, the rules, and the computer networks.

20. (currently amended) A method for analyzing a packet using a firewall which creates a plurality of trust levels for a plurality of computer networks, the method comprising:

using a single router containing the firewall to service each of the plurality of computer networks by performing the steps of:

determining the sub-switch location of a packet;
determining a source of the packet;
determining a destination of the packet;

Attorney Docket No. AUS920030685US1
Serial No. 10/682,402

determining if the packet is attempting to go to a higher trust level; and
responsive to a determination that the packet is not attempting to go to a higher trust
level, permitting the packet;

wherein a trust level is a security level associated with a particular set of rules in the
firewall;

wherein a residence time is the time required for the firewall to analyze and either
permit or deny a packet; and

wherein the trust level reduces the residence time of the packet in the firewall.

21. (original) The method of claim 20, wherein responsive to a determination that the packet is
attempting to go to a higher trust level, the method further comprises:

determining the appropriate rules to use to analyze the packet using the table;

analyzing the packet using the rules;

determining if the packet is permitted under the rules;

responsive to a determination that the rules permit the packet, permitting the packet;

and

responsive to a determination that the rules deny the packet, denying the packet.

22. (original) The method of claim 21 wherein the security program further comprises:

responsive to a determination that the rules do not permit or deny the packet, denying the
packet.

23. (original) The method of claim 20 wherein the firewall further comprises: a table defining the
relationship between the trust levels, the rules, and the computer networks.

Attorney Docket No. AUS920030685US1
Serial No. 10/682,402

24. (currently amended) A program product operable on a computer, the program product comprising:

a computer-usable medium having instructions encoded thereon, for causing a computer to use a single router containing a firewall to service each of a plurality of computer networks by

determining the destination of a packet;

accessing a plurality of rules;

determining an appropriate rule to use to analyze the packet;

analyzing the packet using the appropriate rule;

determining if the packet is permitted under the appropriate rule;

responsive to a determination that the appropriate rule permits the packet, i

permitting the packet; and

responsive to a determination that the appropriate rule denies the packet,

denying the packet;

wherein a trust level is a security level associated with a particular set of rules in the firewall;

wherein a residence time is the time required for the firewall to analyze and either permit or deny a packet; and

wherein the trust level reduces the residence time of the packet in the firewall.

25. (previously amended) The program product of claim 24 further comprising: responsive to a determination that the plurality of rules do not permit or deny the packet, instructions for denying the packet.

Attorney Docket No. AUS920030685US1
Serial No. 10/682,402

26. (previously amended) The program product of claim 24 wherein a table defines the relationship between the trust levels, the rules, and the plurality of computer networks.

27. (currently amended) A program product operable on a computer, the program product comprising:

a computer-usable medium having a plurality of instructions encoded thereon;

wherein the instructions cause a single router containing a firewall to secure each of a plurality of computer networks, and cause an administrator to assign a plurality of trust levels among the plurality of computer networks; to determine the sub-switch location of a packet;

to determine a source of the packet;

to determine a destination of the packet;

to determine if the packet is attempting to go to a higher trust level; and

responsive to a determination that the packet is not attempting to go to a

higher trust level, to permit the packet;

wherein a trust level is a security level associated with a particular set of rules in the firewall;

wherein a residence time is the time required for the firewall to analyze and either permit or deny a packet; and

wherein the trust level reduces the residence time of the packet in the firewall.

28. (original) The program product of claim 27, wherein responsive to a determination that the packet is attempting to go to a higher trust level, the method further comprises:

Attorney Docket No. AUS920030685US1
Serial No. 10/682,402

instructions for determining the appropriate rules to use to analyze the packet using the table;

instructions for analyzing the packet using the rules;

instructions for determining if the packet is permitted under the rules;

responsive to a determination that the rules permit the packet, instructions for permitting the packet; and

responsive to a determination that the rules deny the packet, instructions for denying the packet.

29. (original) The program product of claim 28 wherein the security program further comprises: responsive to a determination that the rules do not permit or deny the packet, instructions for denying the packet.

30. (original) The program product of claim 27 wherein the firewall further comprises: a table defining the relationship between the trust levels, the rules, and the computer networks.

31. (currently amended) A firewall capable of creating a plurality of trust levels for a plurality of computer networks comprising:

a router containing the firewall;

a plurality of rules;

a table defining the relationship between the trust levels, the rules, and the computer networks;

a configuration program, wherein the configuration program allows a user to add, delete, or modify the rules and trust levels in the table;

a security program, wherein the security program analyzes a packet and determines if the rules permit or deny the packet, the security program comprising:

Attorney Docket No. AUS920030685US1
Serial No. 10/682,402

instructions for determining the destination of the packet;
instructions for determining the appropriate rules to use to analyze the packet
using the table;
instructions for analyzing the packet using the rules;
instructions for determining if the packet is permitted under the rules;
responsive to a determination that the rules permit the packet, instructions for
permitting the packet;
responsive to a determination that the rules deny the packet, instructions for
denying the packet; and
responsive to a determination that the rules do not permit or deny the packet,
instructions for denying the packet;
wherein only the firewall is used to protect each of the plurality of computer
networks;
wherein a trust level is a security level associated with a particular set of rules
in the firewall;
wherein a residence time is the time required for the firewall to analyze and
either permit or deny a packet; and
wherein the trust level reduces the residence time of the packet in the
firewall.

32. canceled.